ELSEVIER
Journal of Pure and Applied Algebra 132 (1998) 309–315
JOURNAL OF PURE AND APPLIED ALGEBRA

On generators of polynomial algebras in two commuting or non-commuting variables

Vladimir Shpilrain [a], Jie-Tai Yu [b,*,1]

[a] Department of Mathematics, University of California, Santa Barbara, CA 93106, USA
[b] Department of Mathematics, University of Hong Kong, Pokfulam Road, Hong Kong

Communicated by J. Rhodes; received 13 September 1996; received in revised form 30 April 1997

Abstract

An element of a free associative algebra $A_2 = K\langle x_1, x_2\rangle$ is called primitive if it is an automorphic image of x_1. We address the problem of detecting primitive elements of A_2: we present an algorithm that distinguishes primitive elements, and also give a couple of very handy necessary conditions for primitivity that allow one to rule out many sorts of non-primitive elements of A_2 just by inspection. We also give a structural description of the automorphism groups $Aut(A_2)$ and $Aut(P_2)$ (where $P_2 = K[x_1, x_2]$ is the polynomial algebra in two variables over the same ground field K) which is different from previously known descriptions. © 1998 Elsevier Science B.V. All rights reserved.

AMS Classification: Primary 16W20; secondary 13B25; 17C05

1. Introduction

Let $P_2 = K[x_1, x_2]$ be the polynomial algebra of rank 2 over a field K, and $A_2 = K\langle x_1, x_2\rangle$ the free associative algebra of rank 2 over the same ground field.

It is well known that the automorphism groups $Aut(P_2)$ and $Aut(A_2)$ are isomorphic, an isomorphism $Aut(A_2) \to Aut(P_2)$ being just the natural abelianization. This is due to Makar–Limanov [7] (for $K = \mathbf{C}$) and Czerniakiewicz [3] (for an arbitrary ground field). See also [2, Theorem 9.3].

Furthermore, there is a description of the group $Aut(P_2)$ as a free product with amalgamation due to Shafarevich [9]; see also [2, Theorem 8.6, 5,12] and references thereto.

* Corresponding author. E-mail: yujt@hkusua.hku.hk.
1 Partially supported by RGC Fundable Grant 344/024/0001 and CRCG Grant 337/024/0001.

PII: S0022-4049(97)00134-5

All these results reduce the structure of the group $Aut(P_2)$ to that of smaller groups of automorphisms. In this note, we show that a simple argument leads to a somewhat different group-theoretic description of $Aut(P_2)$ (hence of $Aut(A_2)$) – we use the additive group of the ground field K as a "building block", and then apply various group-theoretic constructions.

We call an automorphism $\varphi \in Aut(P_2)$ an IL-*automorphism* if it is Identical on the Linear part, i.e., if it takes x_i to $x_i + p_i$, where the polynomials p_i, $i = 1,2$, do not have monomials of degree less than 2. A similar definition applies to automorphisms of A_2. Denote the groups of IL-automorphisms of P_2 and A_2 by $Aut_{\mathrm{IL}}(P_2)$ and $Aut_{\mathrm{IL}}(A_2)$, respectively. The subgroup $Aut^{\mathrm{e}}_{\mathrm{IL}}(P_2)$ (or $Aut^{\mathrm{e}}_{\mathrm{IL}}(A_2)$) is generated by *elementary* IL-automorphisms of the form $\{x_1 \to x_1 + f(x_2);\ x_2 \to x_2\}$ and $\{x_1 \to x_1;\ x_2 \to x_2 + f(x_1)\}$, where the one-variable polynomials f do not have monomials of degree less than 2.

Furthermore, let $Aut^0(P_2)$ (respectively, $Aut^0(A_2)$) denote the group of *augmentation-preserving* automorphisms of P_2 (or A_2); these are automorphisms of the form $x_i \to x_i + p_i$, where polynomials p_i, $i = 1,2$, have zero constant terms. Then we have the following.

Theorem 1.1. *Let K be an arbitrary ground field. The group $Aut^0(A_2)$ is a semidirect product of $Aut_{\mathrm{IL}}(A_2)$ and $\mathrm{GL}_2(K)$ (the subgroup $Aut_{\mathrm{IL}}(A_2)$ being normal in $Aut^0(A_2)$, and $\mathrm{GL}_2(K)$ a retract). The group $Aut_{\mathrm{IL}}(A_2)$ is the normal closure (in the group $Aut^0(A_2)$) of $Aut^{\mathrm{e}}_{\mathrm{IL}}(A_2)$. This latter group is isomorphic to the free product $(K^+)^\infty \star (K^+)^\infty$, where $(K^+)^\infty$ is the direct sum of countably many copies of the additive group K^+ of the field K.*

All these statements remain valid upon replacing A_2 with P_2. Thus, group-theoretic properties of the groups $Aut^{\mathrm{e}}_{\mathrm{IL}}(P_2)$ and $Aut^{\mathrm{e}}_{\mathrm{IL}}(A_2)$ (and these are the main building blocks of $Aut(P_2)$ and $Aut(A_2)$, respectively) are determined (to some extent) by properties of the additive group of the ground field K which is usually well understood.

Our further goal is to distinguish primitive elements of the algebra A_2 (an element $u \in A_2$ is called *primitive* if it is an automorphic image of x_1; or, in other words, if there is a generating set $\{u, v\}$ of A_2).

Based on the aforementioned isomorphism between $Aut(P_2)$ and $Aut(A_2)$, and also on our recent result [11] on detecting generators of P_2, we are able to prove the following.

Theorem 1.2. *There is an algorithm that distinguishes primitive elements of the algebra A_2 over a field of characteristic* 0.

Here we assume that we are able to perform calculations in the ground field K, which basically means that, given two elements of K, we can decide whether or not they are equal.

Note that there is a very simple "commutator test" for deciding if a given *pair* of elements generates the algebra A_2, see [4]. The problem of distinguishing primitive elements is obviously more difficult, yet our algorithm itself is fairly simple.

Furthermore, driven by the desire to reveal *non-primitivity* of an element of A_2 just by inspection, we present a couple of very transparent *necessary* conditions for an element of A_2 to be primitive.

Denote by J_2 the *free special Jordan algebra* of rank 2. This is a (non-associative) unital K-algebra generated by the elements x_1 and x_2 of A_2 with respect to the binary operation $x \circ y = \frac{1}{2}(xy + yx)$. To avoid a restriction $char\, K \neq 2$, one can consider a somewhat less user-friendly definition of J_2 upon replacing the binary operation given above by two operations: $x \to x^2$ and $(x, y) \to xyx$.

Then we have the following.

Proposition 1.3. *For an arbitrary ground field* K:

(i) *The algebra* J_2 *is invariant under any automorphism of* A_2.

(ii) *The group* $Aut(J_2)$ *is isomorphic to the group* $Aut(A_2)$ (*and, consequently, to* $Aut(P_2)$).

Corollary 1.4. *If* $u \in A_2$ *is a primitive element of* A_2, *then* $u \in J_2$.

This Corollary gives a very convenient criterion for an element of A_2 to be primitive. Indeed, elements of J_2 are characterized among the elements of A_2 as follows (see [1] or [6]). Define an anti-automorphism $\leftarrow$ of A_2 which re-writes every monomial backwards. For example, $(x_1x_2)^{\leftarrow} = x_2x_1$; $(x_1x_2x_1x_2^2)^{\leftarrow} = x_2^2x_1x_2x_1$, etc. Then $\leftarrow$ is extended to the whole A_2 by linearity. The elements $u \in A_2$ for which $u^{\leftarrow} = u$, are called *palindromic*. Then we have [1]

an element $u \in A_2$ belongs to J_2 if and only if it is palindromic.

Thus, our Corollary 1.4 gives a very convenient necessary (but not sufficient) condition for primitivity.

Corollary 1.5. *Primitive elements of* A_2 *are palindromic.* (*Which means, incidentally, that every* homogeneous component *of a primitive element is palindromic.*)

This condition is quite sensitive since the algebra J_2 is very small compared to the enveloping algebra A_2.

We give here one more necessary condition for primitivity in A_2 based on a result of [10]. Denote by Δ the augmentation ideal of A_2, i.e., the set of elements without constant terms. Every element $u \in \Delta$ has a unique expression of the form $u = d_1(u) \cdot x_1 + d_2(u) \cdot x_2$ (see e.g. [2]). The elements $d_i(u)$ are called (partial) Fox derivatives of u. Then we have the following.

Proposition 1.6. *If* $u \in \Delta$ *is a primitive element of* A_2, *then*

$$d_2(u) \cdot (d_1(u))^{\leftarrow} = d_1(u) \cdot (d_2(u))^{\leftarrow}.$$

In other words, the element $d_2(u) \cdot (d_1(u))^{\leftarrow}$ *is palindromic.*

This condition is also not sufficient for primitivity, but it complements the condition of Corollary 1.5 nicely. For example, the element $x_1 + x_1x_2 + x_2x_1$ passes the test of Corollary 1.5, but not of Proposition 1.6.

2. Preliminaries

We start by fixing some notation. For an automorphism $\varphi \in Aut(P_2)$ that takes x_i to p_i, $i=1,2$, the Jacobian matrix is defined as follows: $J_\varphi = (d_j(p_i))_{1\le i,j\le 2}$, where d_j is "usual" Leibnitz partial derivation.

Similarly, if $\varphi \in Aut(A_2)$ takes x_i to u_i, $i=1,2$, then $J_\varphi = (d_j(u_i))_{1\le i,j\le 2}$, but this time, d_j denotes partial Fox derivation. (We use the same notation for Leibnitz and Fox derivations without ambiguity.)

There is a useful product rule for the Jacobian matrices (it is the same in the commutative and the non-commutative situation)

$$J_{\varphi\psi} = \psi(J_\varphi) \cdot J_\psi. \tag{1}$$

(When we write a product $\varphi\psi$, that means ψ is applied first. When we write $\psi(J_\varphi)$, that means ψ is applied to each entry of J_φ).

We are going to need some more background on Fox derivatives (a general reference here is [2]).

The augmentation ideal Δ of the algebra A_2 is a free left and right A_2-module with a free basis (x_1,x_2), so that for any $u \in \Delta$, there is a unique expression of the form $u = d_1(u)\cdot x_1 + d_2(u)\cdot x_2$ as well as of the form $u = x_1 \cdot D_1(u) + x_2 \cdot D_2(u)$. The elements $D_j(u)$ are called right Fox derivatives of u, and $d_j(u)$ (left) Fox derivatives.

One can extend these derivations linearly to the whole A_2 by setting $D_i(1) = d_i(1) = 0$.

Then the result of [10] yields the following.

Lemma 2.1. *Let u be a primitive element of A_2. Then $d_2(u)\cdot D_1(u) - d_1(u)\cdot D_2(u) = 0$.*

Proof. It was proved in [10] that for an automorphism $\varphi \in Aut(A_2)$ that takes x_i to y_i, $i=1,2$, one has

$$\begin{pmatrix} D_2(y_2) & -D_2(y_1) \\ -D_1(y_2) & D_1(y_1) \end{pmatrix} \cdot \begin{pmatrix} d_1(y_1) & d_2(y_1) \\ d_1(y_2) & d_2(y_2) \end{pmatrix} = c \cdot I,$$

where $c \in K^*$, and I is the identity matrix.

It follows from a result of Cohn [2] (every right-invertible square matrix over a free ideal ring is also left invertible) that

$$\begin{pmatrix} d_1(y_1) & d_2(y_1) \\ d_1(y_2) & d_2(y_2) \end{pmatrix} \cdot \begin{pmatrix} D_2(y_2) & -D_2(y_1) \\ -D_1(y_2) & D_1(y_1) \end{pmatrix} = c \cdot I,$$

whence $d_1(y_1)\cdot(-D_2(y_1)) + d_2(y_1)\cdot D_1(y_1) = 0$. This proves the claim. □

We also need Nagao's theorem [8] (see also [12]):

Theorem 2.2 (Nagao [8]). *$GL_2(K[t]) = GL_2(K) \star_{UT_2(K)} UT_2(K[t])$, where $K[t]$ is the polynomial algebra in one variable t over K, and UT_2 is a group of 2×2 upper triangular matrices. The statement is also valid upon replacing the upper triangular group with the lower triangular group.*

3. Proofs

Proof of Theorem 1.1. We start with the first statement. It is straightforward to verify that $Aut_{\mathrm{IL}}(A_2)$ is a normal subgroup of $Aut^0(A_2)$. Also, it is obvious that the intersection of $Aut_{\mathrm{IL}}(A_2)$ with the group of *linear* automorphisms is trivial. This means the group $Aut^0(A_2)$ is a semidirect product of $Aut_{\mathrm{IL}}(A_2)$ and $GL_2(K)$. (The fact that $Aut^0(A_2)$ is the *product* of those two subgroups, follows from the results of [3].)

It follows that every automorphism $\varphi \in Aut^0(A_2)$ can be written in the form $\varphi = \lambda\psi$, where λ is a linear automorphism, and $\psi \in Aut_{\mathrm{IL}}(A_2)$.

On the other hand, by the results of [3], every automorphism $\varphi \in Aut^0(A_2)$ can be written as a product of linear automorphisms and elementary automorphisms of the form $\{x_1 \to x_1 + c \cdot x_2^m;\ x_2 \to x_2\}$ and $\{x_1 \to x_1;\ x_2 \to x_2 + c \cdot x_1^m\}$ for all possible $c \in K$ and $m \geq 2$. These elementary automorphisms clearly belong to the group $Aut_{\mathrm{IL}}^{\mathrm{e}}(A_2)$. Now a standard re-writing process (based on the equality $abc = b(b^{-1}ab)c = ba^bc$) in combination with what is said in the previous paragraph, proves the second statement of Theorem 1.1.

Now, we are going to prove the claim about the group $G = Aut_{\mathrm{IL}}^{\mathrm{e}}(A_2)$.

Denote two copies of $(K^+)^\infty$ by A and B, and their natural components by $\{A_2, A_3, \ldots\}$ and $\{B_2, B_3, \ldots\}$, respectively (we deliberately start with index 2 for subsequent notational convenience). All the groups A_k and B_k are isomorphic to the group K^+.

We are now going to define a mapping τ from $A \star B$ into G on these components; the fact that a mapping like that can be extended to a homomorphism of groups, follows from the universal properties of the group-theoretic constructions involved.

Let τ take $a_i \in A_i$ to the following automorphism $\alpha_i : x_1 \to x_1 + a_i \cdot x_2^i;\ x_2 \to x_2$. Then, let τ take $b_i \in B_i$ to the automorphism $\beta_i : x_1 \to x_1;\ x_2 \to x_2 + b_i \cdot x_1^i$. Everywhere, $i \geq 2$.

First we prove that τ is injective. By way of contradiction, suppose, say, $\hat{\alpha}_1\hat{\beta}_1 \cdot \cdots \cdot \hat{\alpha}_k\hat{\beta}_k = id$, where $\hat{\alpha}_i$ (or $\hat{\beta}_i$) is a product of finitely many α_{i_j} (or β_{i_j}), and id is the identity mapping. We assume that all $\hat{\alpha}_i$, $\hat{\beta}_i$ are non-identity mappings.

Then applying the product rule (1) for the Jacobian matrices yields

$$\psi_1(J_{\hat{\alpha}_1}) \cdot \psi_2(J_{\hat{\beta}_1}) \cdot \cdots \cdot \psi_k(J_{\hat{\alpha}_k}) \cdot J_{\hat{\beta}_k} = I, \tag{2}$$

where $\psi_j \in Aut_{\mathrm{IL}}^{\mathrm{e}}(A_2)$ are appropriate automorphisms (of no particular importance to us), and I is the identity matrix.

All the matrices $\psi_j(J_{\hat{\alpha}_i})$ are obviously upper triangular, and the matrices $\psi_j(J_{\hat{\beta}_i})$ are lower triangular. Furthermore, none of them is the identity matrix, and, moreover, none of them belongs to the group $UT_2(K)$ since none of the $J_{\hat{\alpha}_i}$, $J_{\hat{\beta}_i}$ does.

Consider now the abelianization $x_1 \to t$; $x_2 \to t$. An abelianized matrix $\psi_j(J_{\hat{\alpha}_i})^a$ or $\psi_j(J_{\hat{\beta}_i})^a$ does not belong to $UT_2(K)$ unless it is the identity matrix.

Indeed, any off-diagonal entry in a matrix $\psi_j(J_{\hat{\alpha}_i})$, say, has the form $\psi_j(f(x_2))$, where f is some (non-constant!) one-variable polynomial, so that $\psi_j(f(x_2))^a = f(\psi_j(x_2)^a) \notin K$ since $\psi_j(x_2)$ must be either non-constant or zero, so its abelianization is either non-constant or zero, too.

Applying Nagao's theorem (see Theorem 2.2) to the abelianized equality (2) yields a contradiction (note that $J_{\hat{\beta}_k} \neq I$ in (2)) which completes the proof of τ being injective.

The fact that τ is surjective follows from the very definition of the group $Aut^{\mathrm{e}}_{\mathrm{IL}}(A_2)$. Thus, τ is an isomorphism. □

The corresponding statements about automorphisms of P_2 can now be easily deduced from the fact that the groups $Aut^0(P_2)$ and $Aut^0(A_2)$ are naturally isomorphic. We omit the details.

Proof of Theorem 1.2. Let $u \in A_2$. Denote by $u^a \in P_2$ the abelianization of u. If u^a is *not* a coordinate polynomial of P_2, then u is obviously not a primitive element of A_2. Note that we can decide whether or not u^a is coordinate using a (very simple) algorithm from [11]. This latter algorithm was constructed only in the situation when $char\, K = 0$ – that is why we need this restriction here.

Let u^a be a coordinate polynomial of P_2. Using again a procedure from [11], we can find a sequence of elementary automorphisms that takes x_1 to u^a. Apply the same sequence to x_1, but in the algebra A_2 (we identify elementary automorphisms of P_2 and A_2 by means of the natural isomorphism mentioned in the Introduction). If we arrive at the element u, then u is obviously primitive. What is not so obvious, is what happens if we arrive at a different element, call it v.

We are going to show now that if $v \neq u$, then u is not primitive in A_2. By way of contradiction, suppose u is primitive. Let $\psi \in Aut(A_2)$ take x_1 to u. Furthermore, let $\varphi(x_1) = v$ in A_2, so that $\varphi(x_1) = u^a$ in P_2 (we use the same letter for an automorphism $\varphi \in Aut(A_2)$ and its natural image in $Aut(P_2)$).

Since $u^a = v^a$, this yields $\varphi(x_1) = \psi(x_1)$ in P_2. By [2, Theorem 8.5], this implies $\varphi = \psi\alpha$ for some $\alpha \in Aut(P_2)$ of the form $\{x_1 \to x_1;\ x_2 \to x_2 + f(x_1)\}$. This means $\varphi = \psi\alpha$ also in $Aut(A_2)$.

But α, as well as its fellow-automorphism of A_2, does not change x_1, hence $\psi(\alpha((x_1)) = \psi(x_1)$ both in P_2 and A_2. Therefore, we have in A_2: $v = \varphi(x_1) = \psi(\alpha((x_1)) = \psi(x_1) = u$, a contradiction.

Therefore, u was not primitive in A_2, and this completes the proof of Theorem 1.2. □

Proof of Proposition 1.3. (i) Since any automorphism of A_2 respects the operations of J_2, it is sufficient to show that x_1 and x_2 are carried into J_2 by any linear automorphism of A_2 and by any automorphism of the form $\{x_1 \to x_1 + cx_2^k;\ x_2 \to x_2\}$ and $\{x_1 \to x_1;\ x_2 \to x_2 + cx_1^k\}$, $k \geq 2$, $c \in K$.

For linear automorphisms, this is obvious since any linear automorphism carries the K-linear span of $\{x_1, x_2\}$ into itself.

For other automorphisms above this is clear, too, since $x_1^k, x_2^k \in J_2$ for any k.

(ii) As we have just seen, every automorphism of A_2 induces an automorphism of J_2; this mapping is obviously injective. Conversely, if φ is an automorphism of J_2, then $\varphi(x_1)$ and $\varphi(x_2)$ generate the algebra J_2, hence they also generate A_2. Therefore, φ is induced by an automorphism of A_2. The result follows. □

Proof of Proposition 1.6. We are going to show that there is the following "mirror symmetry" between left and right Fox derivatives for any $u \in A_2$ (it actually holds in a free associative algebra of arbitrary rank)

$$D_i(u^{\leftarrow}) = (d_i(u))^{\leftarrow}. \tag{3}$$

Without loss of generality, we can assume $u \in \Delta$, so let $u = \sum d_i(u) \cdot x_i$. Then $u^{\leftarrow} = \sum x_i \cdot (d_i(u))^{\leftarrow}$, hence $(d_i(u))^{\leftarrow} = D_i(u^{\leftarrow})$ proving the equality (3). □

Combining (3) with Lemma 2.1 and Corollary 1.5 yields the result. □

Acknowledgements

We are grateful to Andrew Campbell and to the referee for helpful comments.

References

[1] P.M. Cohn, On homomorphic images of special Jordan algebras, Can. J. Math. 6 (1954) 253–264.
[2] P.M. Cohn, Free Rings and Their Relations, Academic Press, New York, 1985.
[3] A.J. Czerniakiewicz, Automorphisms of a free associative algebra of rank 2, I, II, Trans. Amer. Math. Soc. 160 (1971) 393–401; 171 (1972) 309–315.
[4] W. Dicks, A commutator test for two elements to generate the free algebra of rank two, Bull. London Math. Soc. 14 (1982) 48–51.
[5] W. Dicks, Automorphisms of the polynomial ring in two variables, Publ. Sec. Mat. Univ. Autonoma Barcelona 27 (1983) 155–162.
[6] N. Jacobson, Structure and Representation of Jordan Algebras, Colloq. Publ. 39, American Mathematical Society, Providence, 1968.
[7] L.G. Makar-Limanov, On automorphisms of free algebra with two generators, Funk. Analiz i ego Prilozh. 4 (1970) (3), 107–108 (Russian).
[8] H. Nagao, On GL(2, $K[x]$), J. Inst. Polytech. Osaka City Univ. Ser. A 10 (1959) 117–121.
[9] I.R. Shafarevich, On some infinite-dimensional groups, Rend. Mat. Appl. 25 (1966) 208–212.
[10] V. Shpilrain, An inverse function theorem for free associative algebras of rank two, J. Pure Appl. Algebra 83 (1992) 23–26.
[11] V. Shpilrain, J.-T. Yu, Polynomial automorphisms and Gröbner reduction, preprint.
[12] D. Wright, The amalgamated free product structure of $GL_2(k[X_1, \ldots, X_n])$ and the weak Jacobian theorem for two variables, J. Pure Appl. Algebra 12 (1978) 235–251.